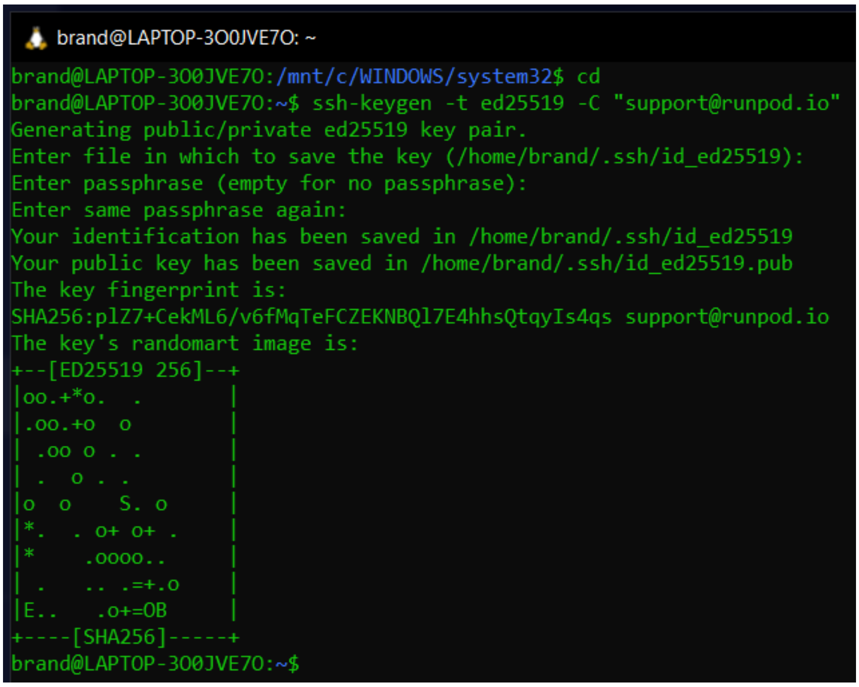
Use SSH

The basic terminal SSH access that RunPod exposes is not a full SSH connection and, therefore, does not support commands like SCP. If you want to ha

Setup

1. Generate your public/private SSH key pair on your local machine with `ssh-keygen -t ed25519 -C "your_email@example.com"`. This will sav

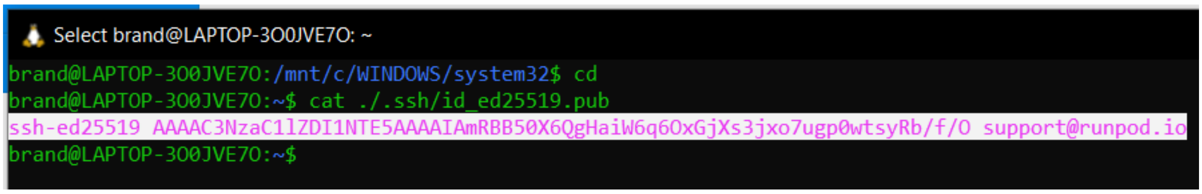
> **NOTE**
>
> if you're using command prompt in Windows rather than the Linux terminal or WSL, your public/private key pair will be saved to `C:\users\{you`



brand@LAPTOP-3O0JVE7O: ~

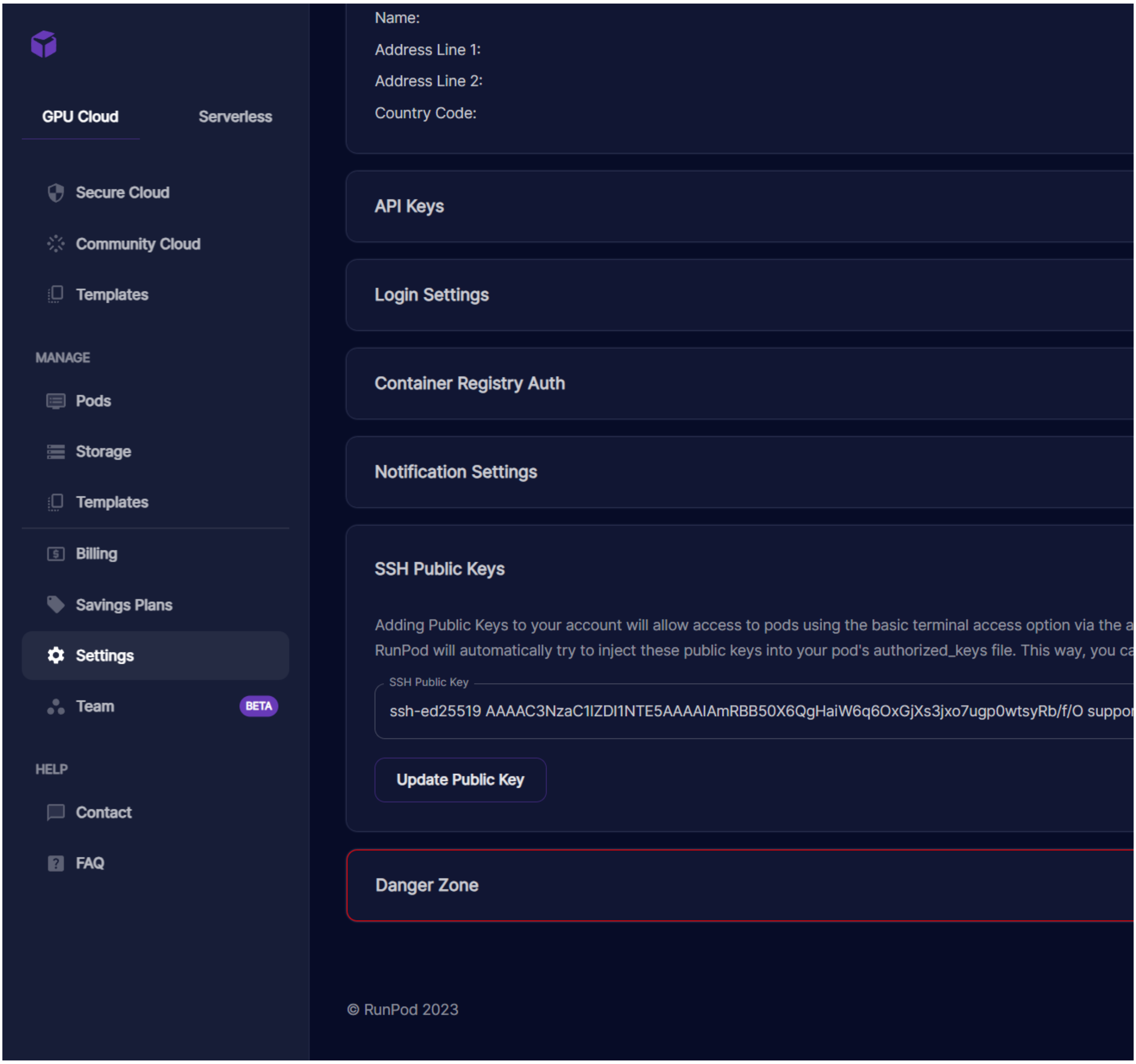
```
brand@LAPTOP-3O0JVE7O:/mnt/c/WINDOWS/system32$ cd
brand@LAPTOP-3O0JVE7O:~$ ssh-keygen -t ed25519 -C "support@runpod.io"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/brand/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/brand/.ssh/id_ed25519
Your public key has been saved in /home/brand/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:plZ7+CekML6/v6fMqTeFCZEKNBQl7E4hhsQtqyIs4qs support@runpod.io
The key's randomart image is:
+--[ED25519 256]--+
|oo.+*o.  .       |
|.oo.+o  o        |
| .oo o . .       |
| .  o . .        |
|o  o    S. o     |
|*.   . o+ o+ .   |
|*    .oooo..     |
| .   .. .=+.o    |
|E..   .o+=OB     |
+----[SHA256]-----+
brand@LAPTOP-3O0JVE7O:~$
```

2. Add your public key to your RunPod user settings.



Select brand@LAPTOP-3O0JVE7O: ~

```
brand@LAPTOP-3O0JVE7O:/mnt/c/WINDOWS/system32$ cd
brand@LAPTOP-3O0JVE7O:~$ cat ./.ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAmRBB50X6QgHaiW6q6OxGjXs3jxo7ugp0wtsyRb/f/O support@runpod.io
brand@LAPTOP-3O0JVE7O:~$
```



Name:

Address Line 1:

Address Line 2:

Country Code:

SSH Public Keys

Adding Public Keys to your account will allow access to pods using the basic terminal access option via the a RunPod will automatically try to inject these public keys into your pod's authorized_keys file. This way, you ca

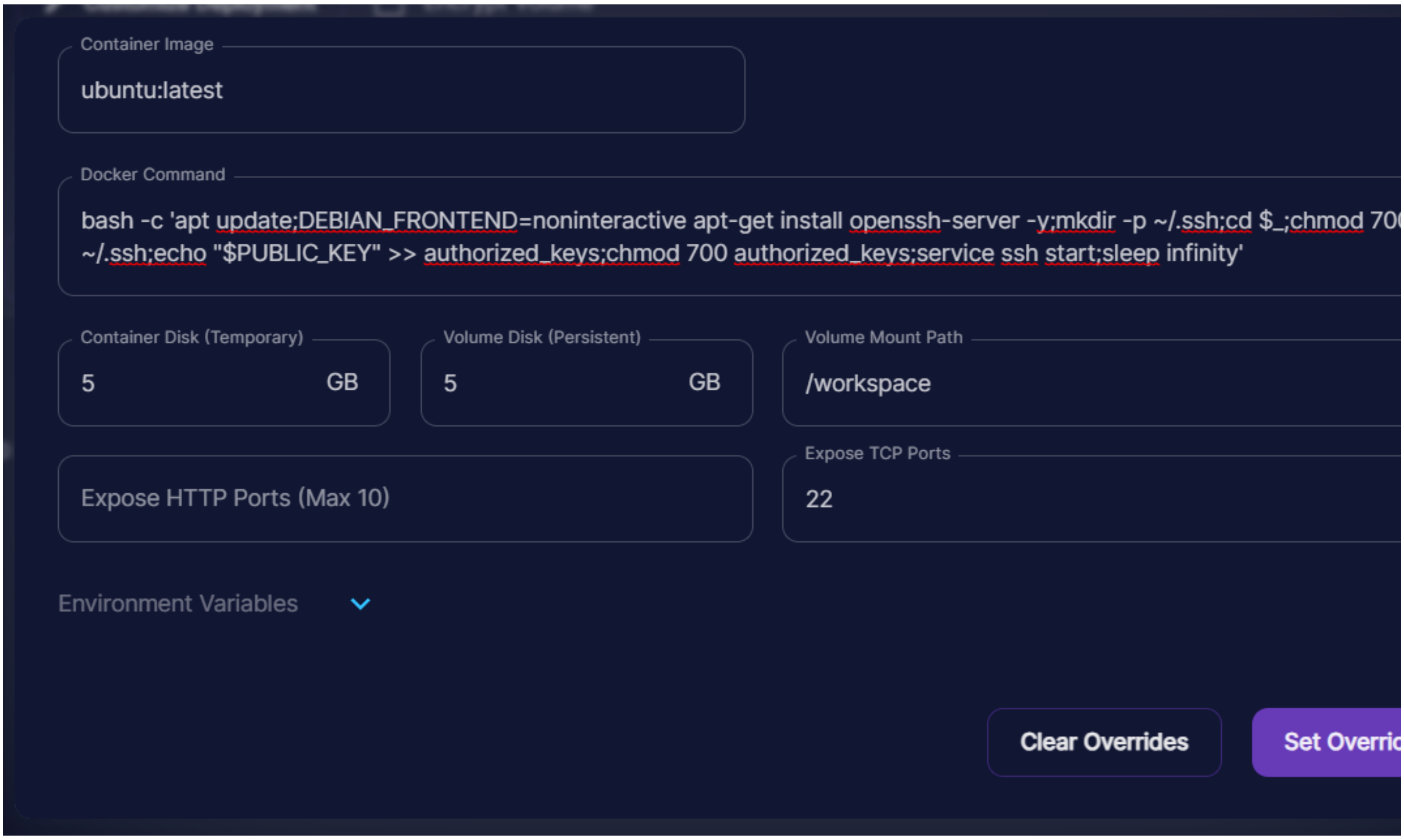
SSH Public Key

ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAmRBB50X6QgHaiW6q6OxGjXs3jxo7ugp0wtsyRb/f/O suppo

3. Start your Pod. Make sure of the following things:

- Your Pod supports a public IP, if you're deploying in Community Cloud.
- An SSH daemon is started. If you're using a RunPod official template such as RunPod Stable Diffusion, you don't need to take any additional steps. I an existing start command, replace `sleep infinity` at the end with your existing command:

```
bash -c 'apt update;DEBIAN_FRONTEND=noninteractive apt-get install openssh-server -y;mkdir -p ~/.ssh;cd $_;chmod 700
```



Container Image: ubuntu:latest

Docker Command:

```
bash -c 'apt update;DEBIAN_FRONTEND=noninteractive apt-get install openssh-server -y;mkdir -p ~/.ssh;cd $_;chmod 70
~/.ssh;echo "$PUBLIC_KEY" >> authorized_keys;chmod 700 authorized_keys;service ssh start;sleep infinity'
```

Container Disk (Temporary): 5 GB

Volume Disk (Persistent): 5 GB

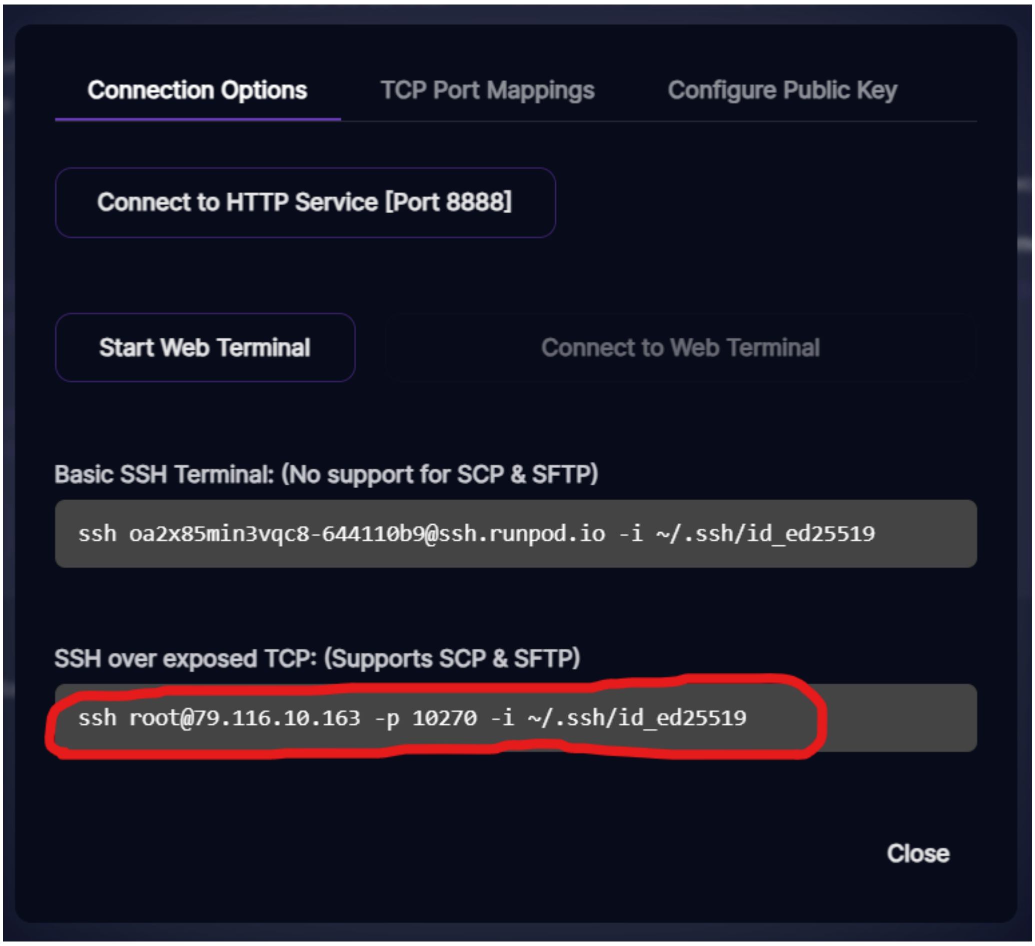
Volume Mount Path: /workspace

Expose HTTP Ports (Max 10)

Expose TCP Ports: 22

Once your Pod is done initializing, you'll be able to SSH into it by running the SSH over exposed TCP command in the Pod's Connection Options menu on

> **NOTE**
>
> - if you're using the Windows Command Prompt rather than the Linux terminal or WSL, and you've used the default key location when generating y SSH command after the `-i` flag to `C:\users\{yourUserAccount}\.ssh\id_ed25519`.
> - If you've saved your key to a location other than the default, specify that path you chose when generating your key pair after the `-i` flag instead.

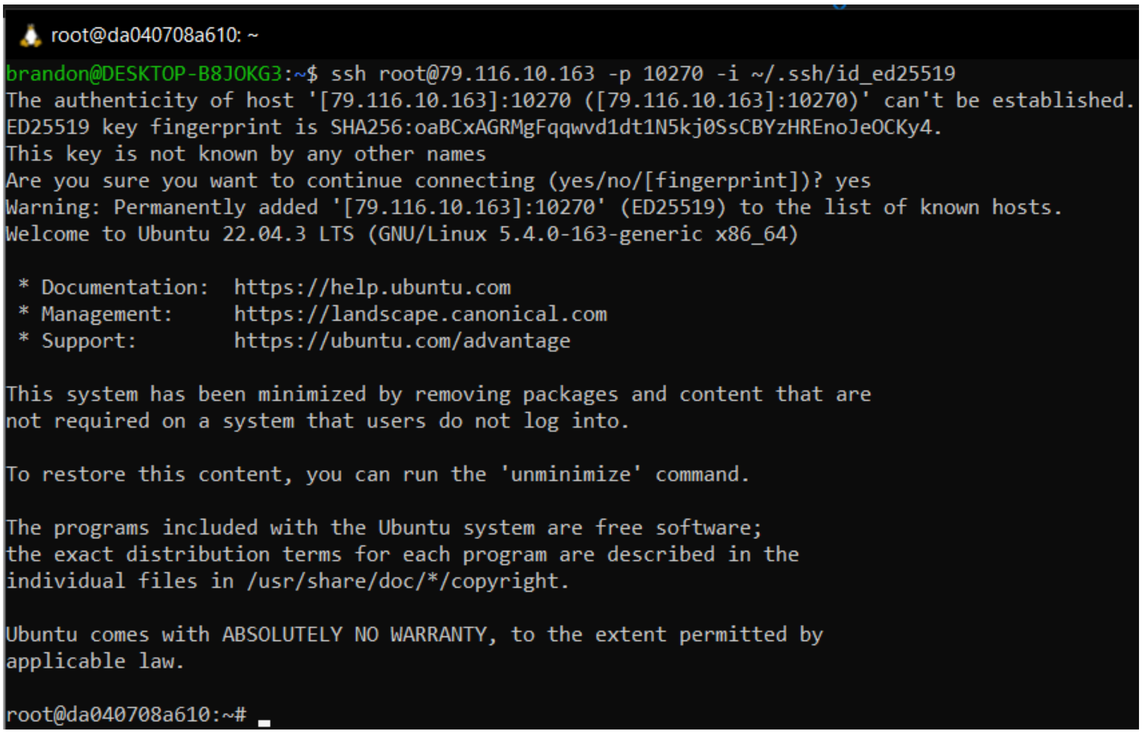


Basic SSH Terminal: (No support for SCP & SFTP)

```
ssh oa2x85min3vqc8-644110b9@ssh.runpod.io -i ~/.ssh/id_ed25519
```

SSH over exposed TCP: (Supports SCP & SFTP)

```
ssh root@79.116.10.163 -p 10270 -i ~/.ssh/id_ed25519
```



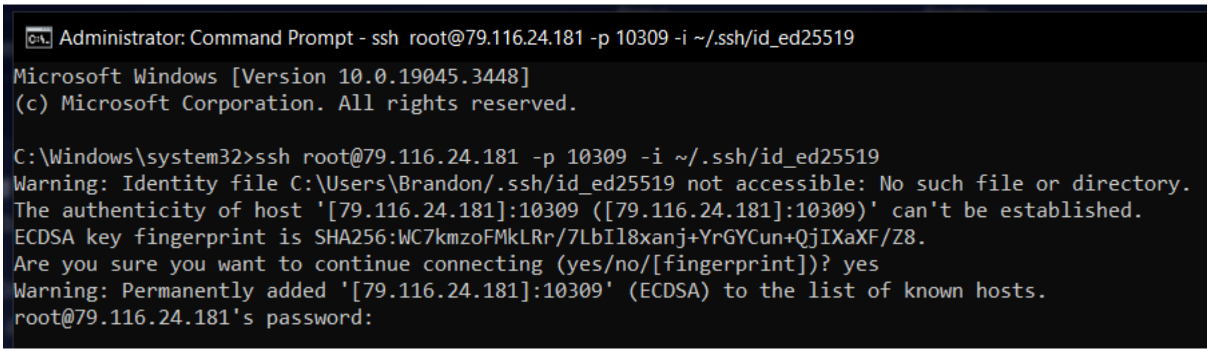
```
brandon@DESKTOP-B8JOKG3:~$ ssh root@79.116.10.163 -p 10270 -i ~/.ssh/id_ed25519
The authenticity of host '[79.116.10.163]:10270 ([79.116.10.163]:10270)' can't be established.
ED25519 key fingerprint is SHA256:oaBCxAGRMgFqqwvd1dt1N5kj0SsCBYzHREnoJeOCKy4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[79.116.10.163]:10270' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.4.0-163-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@da040708a610:~# _
```

What's the SSH password?

If you're being prompted for a password when you attempt to connect, something is amiss. We don't require a password for SSH connections. Some cor

- Copying and pasting the key *fingerprint* (beginning with `SHA256:`) into your RunPod user settings instead of the public key itself (the contents of th
- Omitting the encryption type from the beginning of the key when copying and pasting into your RunPod user settings (i.e., copying the random text,
- Not separating different public keys in your RunPod user settings with a newline between each one (this would result in the first public/private key p

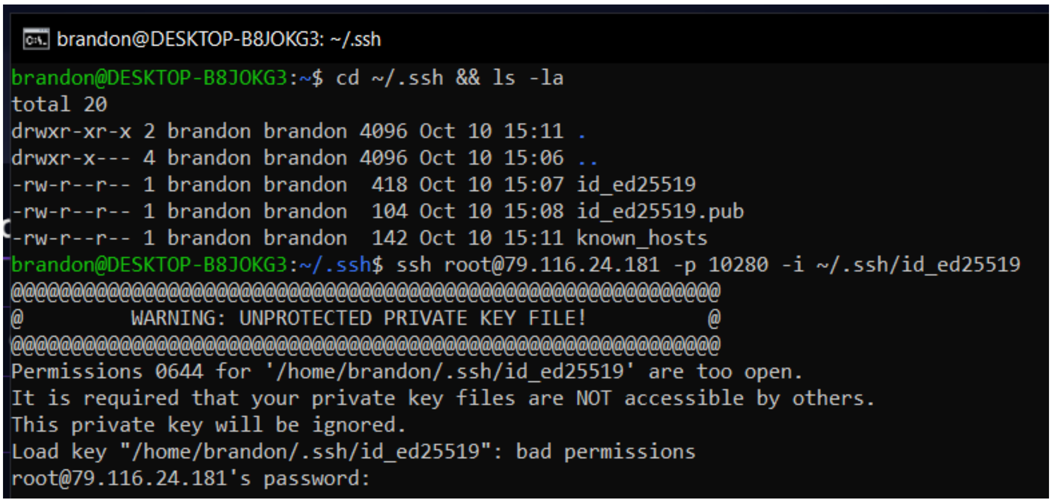
- Specifying an incorrect file path to your private key file:



Administrator: Command Prompt - ssh root@79.116.24.181 -p 10309 -i ~/.ssh/id_ed25519

```
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ssh root@79.116.24.181 -p 10309 -i ~/.ssh/id_ed25519
Warning: Identity file C:\Users\Brandon/.ssh/id_ed25519 not accessible: No such file or directory.
The authenticity of host '[79.116.24.181]:10309 ([79.116.24.181]:10309)' can't be established.
ECDSA key fingerprint is SHA256:WC7kmzoFMkLRr/7LbIl8xanj+YrGYCun+QjIXaXF/Z8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[79.116.24.181]:10309' (ECDSA) to the list of known hosts.
root@79.116.24.181's password:
```

- Attempting to use a private key that other users on the machine have permissions for:



```
brandon@DESKTOP-B8JOKG3:~$ cd ~/.ssh && ls -la
total 20
drwxr-xr-x 2 brandon brandon 4096 Oct 10 15:11 .
drwxr-x--- 4 brandon brandon 4096 Oct 10 15:06 ..
-rw-r--r-- 1 brandon brandon  418 Oct 10 15:07 id_ed25519
-rw-r--r-- 1 brandon brandon  104 Oct 10 15:08 id_ed25519.pub
-rw-r--r-- 1 brandon brandon  142 Oct 10 15:11 known_hosts
brandon@DESKTOP-B8JOKG3:~/.ssh$ ssh root@79.116.24.181 -p 10280 -i ~/.ssh/id_ed25519
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for '/home/brandon/.ssh/id_ed25519' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "/home/brandon/.ssh/id_ed25519": bad permissions
root@79.116.24.181's password:
```

Edit this page